APAC Cybersecurity Fund

The Asia Foundation

Module 3

Software Updates and Business Security

implemented in India by MSME Foundation for MSME Clusters (FMC)

with support from Google.org

Training Module developed under the project **APAC Cybersecurity Fund**

This training module is designed to provide general information and guidance on cybersecurity best practices. While every effort has been made to ensure the accuracy and relevance of the content, the information provided is for educational purposes only and does not constitute professional advice or an exhaustive cybersecurity strategy. By participating in this training, you acknowledge and accept that the information is provided "as is," without any guarantees or warranties of any kind, express or implied. For tailored cybersecurity solutions, please consult with certified experts.

Organized by **The Asia Foundation**

Implemented in India by **The Foundation for MSME Clusters**

Supported by **Google.org**

ℹ Module also available in Hindi, Marathi, Punjabi, Kannada and Telugu

Module developed by **Global Cyber Alliance** & **CyberPeace Foundation**

Module designed by **Chowdhury, Basu & Ray**

Version 1.0 December, 2024

Module 3

Software Updates and Business Security

Manufacturers and software developers regularly update their applications and operating systems to address newly discovered weaknesses or vulnerabilities in their products. These updates will be available for all types of devices (mobile, tablet, laptop, desktop, hotspot, etc.) and apps. Be sure to pay attention no matter what type of devices you use.

These fixes are referred to as software updates or patches and the process is known as patching.

What We Will Talk About

1 SOFTWARE PATCHING IMPROVES YOUR SECURITY.

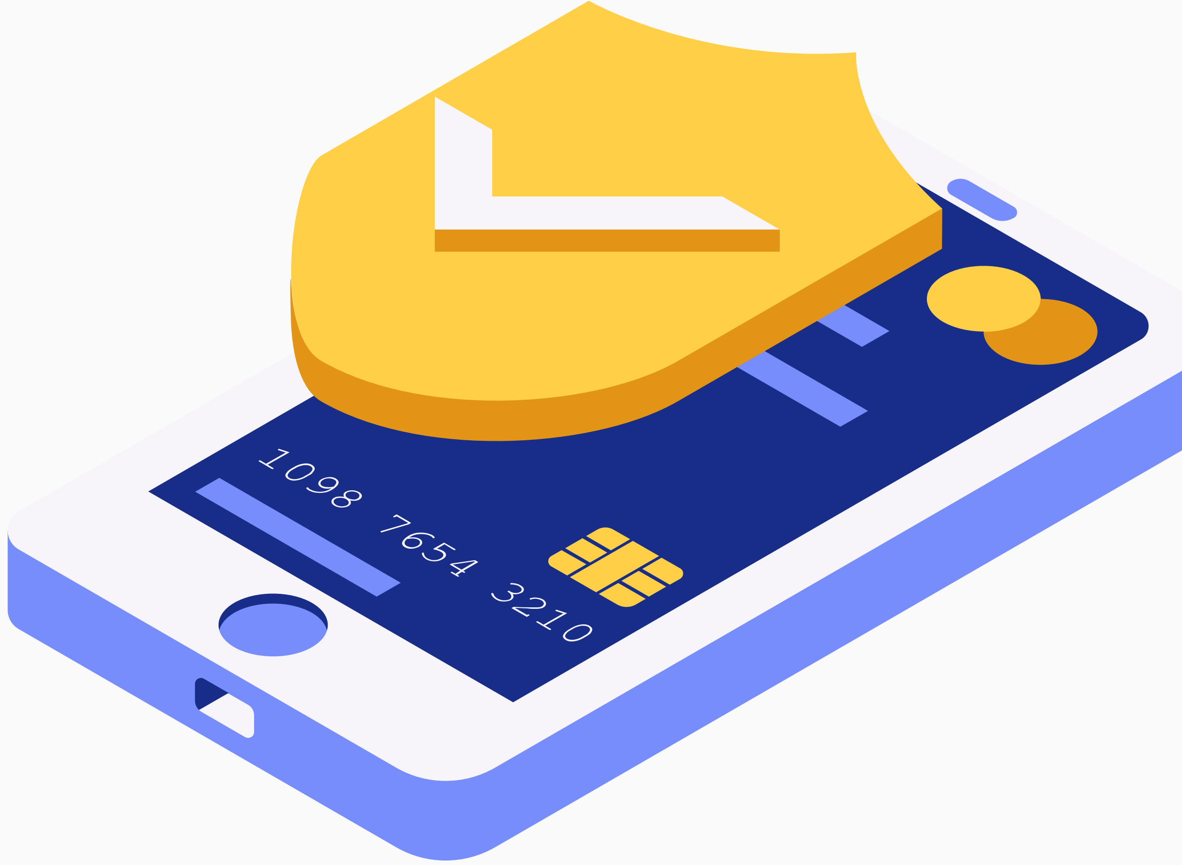
2 DO SECURITY PATCHES EVER STOP BEING MADE?

3 IOT (INTERNET OF THINGS) DEVICES

4 CHECKLIST

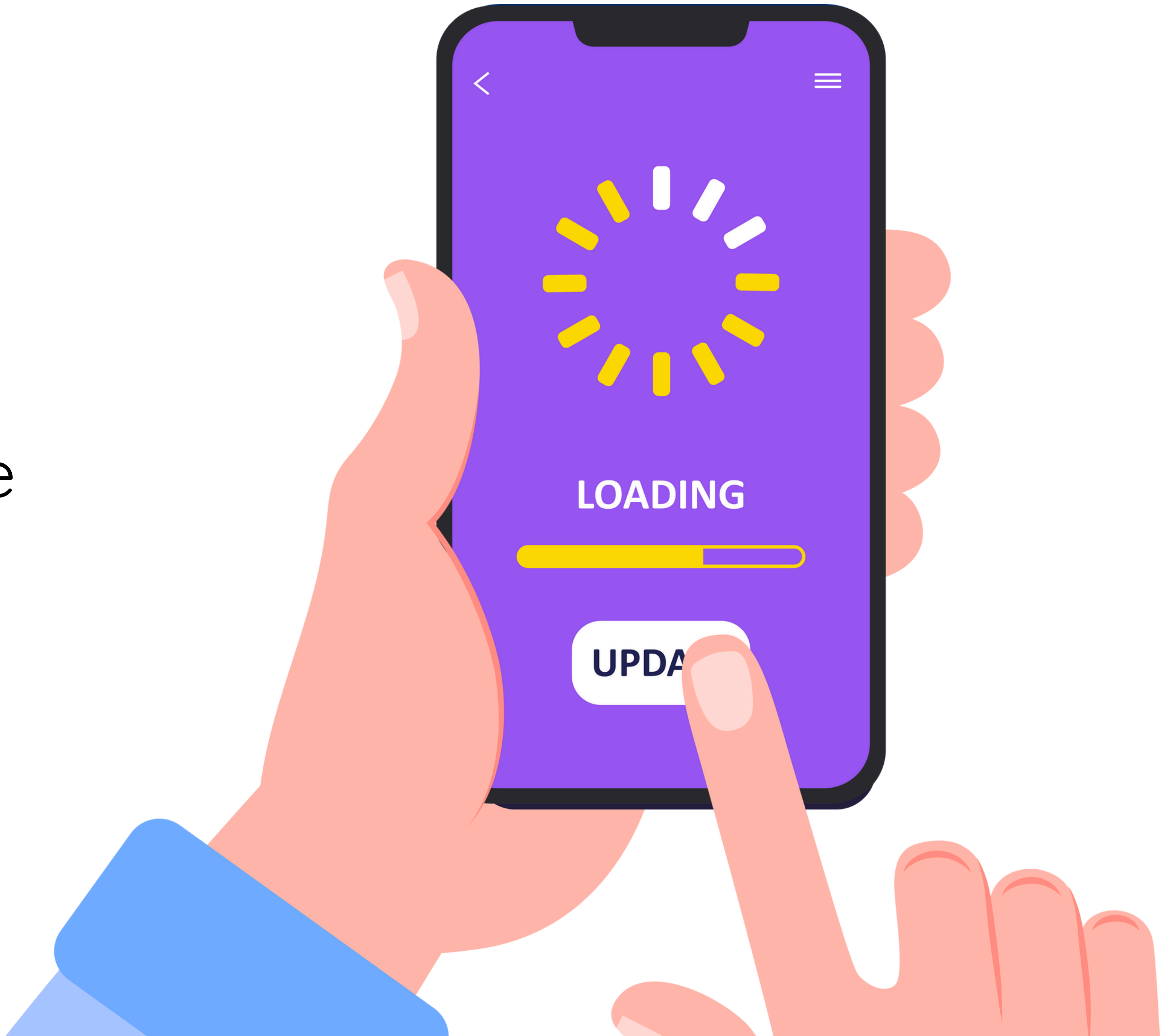
Software patching improves your security.

- Remember, cyber criminals are constantly looking for ways to gain access to systems, accounts, and data.
- A way they do this is by finding a weakness in a configuration or code they can replicate across the entire user base and exploit it to their advantage.
- Patching is critical to your security and should be done as soon as possible.
- It is absolutely critical for patches to be applied quickly and automatically whenever possible to protect your personal and professional data from being compromised.



Here’s a quick snapshot of some other reasons why you need to prioritise your software patches and updates:

- Compliance Issues: Legacy software may not meet current regulatory standards.
- Incompatibility with Modern Systems: Legacy software may not integrate with newer systems.
- Decreased Efficiency and Performance: Older software may be slower and less stable.
- Lack of Vendor Support: Legacy software may no longer receive vendor support.



Some real-world example of how users failing to download a readily-available security patch had devastating effects.

- **IRCTC Breach (2018):** Hackers exploited vulnerabilities in the IRCTC (Indian Railway Catering and Tourism Corporation) booking platform, which was using outdated security measures. Exposed the information of around 200,000 passengers for two years. The vulnerability allowed users to be redirected to a third-party insurer, which exposed their information.
- **Aadhaar Data Breach (2018):** The Aadhaar system, which houses biometric and personal data of over 1.3 billion Indians, suffered data breaches due to insufficient patch management.
- **JustDial Data Breach (2019) :** In 2019, JustDial, a major Indian local search engine, suffered a data breach that exposed over 100 million customer records, including names, phone numbers, email addresses, and physical addresses. The breach occurred due to a vulnerability in their software that allowed unauthorized access to their database. The breach was reportedly linked to an insecure API and inadequate security measures.

Do Security Patches Ever Stop Being Made?

“End of Life” and Software Updates

- All devices and operating systems have an “end of life” date after which they are no longer maintained. After this date, technical support ceases and no further patches are released.

- Using these devices and systems after their "end of life" becomes an immediate and ongoing risk for any newly discovered vulnerabilities. This stop of patching can also happen if a manufacturer ceases trading and no one takes on the development of its product set.

IoT (Internet of Things) Devices

The dramatic growth of Internet of Things (IoT) devices has exponentially increased potential access points for attackers. Many of the IoT devices used on a daily basis have very limited security features or no patching capabilities. This means if a flaw does exist, your network would be open to attack until the device is physically removed or proper security measures are implemented.

IoT devices often face patching limitations due to:

- Device Manufacturer Support: Many IoT manufacturers do not provide ongoing updates for older devices.
- Lack of Standardization: IoT devices often operate on proprietary firmware, which makes regular updates challenging.
- Many IoT devices lack automatic update features, making them vulnerable to attacks. In India, CCTV cameras, smart printers, and eve POS machines often run on outdated software.

Examples Of Outdated Devices Still Being Used In India

- **Windows XP PCs**: Despite Microsoft officially ending support for Windows XP in April 2014, it is still used in several parts of India, particularly in government offices, small businesses, and educational institutions, mainly due to legacy software dependencies.

- **Windows 7 PCs**: Though Microsoft ended support for Windows 7 in January 2020, many businesses and individuals still use it because of the cost and compatibility issues associated with upgrading. Windows 7 is still prevalent in various MSMEs across India.

- **Old Mobile Phones**: Feature phones, especially those running outdated operating systems like Nokia's Series 40 or earlier versions of the Android OS (such as Gingerbread), are still widely used in rural India due to affordability. These devices don't receive updates and are more vulnerable to security threats.

- **Old POS Terminals**: Many small retailers in India still use legacy POS terminals that run on outdated operating systems (Windows CE, Windows XP). These devices may lack modern security features like encryption and secure transaction protocols.

- **Legacy ATM Machines**: Numerous ATMs across India still run on outdated software and hardware that are vulnerable to security threats. These ATMs often run on old operating systems, such as Windows XP or outdated versions of Windows 7, which may not be receiving security updates anymore.

Old applications that are no longer in use and older or outdated equipment (mobile, tablet, laptop, desktop, hotspot, etc.) should be removed or deactivated as quickly as possible to avoid these security risks. These should ideally have been identified and removed/updated while completing your inventory.

Stop using and replace any unsupported systems that have not been upgraded/replaced:

Some systems that have gone end of life that aren't actively being supported/protected:

- **Windows 7** went end of life in **January 2020**
- **Windows XP** went end of life in **April 2014**
- **Windows 10** will be at its end of life **October 14, 2025**

Examples Of Outdated Software Solutions Still Being Used In India

- **Microsoft Office 2007:** Microsoft Office 2007, while still in use in many businesses, no longer receives official support or security patches from Microsoft since 2017. It lacks modern features, compatibility with newer file formats, and suffers from potential vulnerabilities.

- **Outdated Accounting Software**: Many MSMEs in India still use legacy accounting software like Tally ERP 9 (pre-2020 version) and Busy Accounting Software (older versions), which may not be receiving updates or patches, leaving them open to security risks.

- **Adobe Flash Player**: Adobe Flash Player was officially discontinued by Adobe in December 2020. Despite this, some businesses in India continue to use legacy systems or software that rely on Flash for web functionality, exposing themselves to potential security risks as no further updates or support are available.

- **Older ERP Systems**: Many companies continue to use outdated versions of SAP ERP (pre-2015 versions) or Oracle ERP. These older Enterprise Resource Planning systems are prone to vulnerabilities, especially if they haven’t been patched or upgraded in years.

- **Antivirus Software:** Legacy antivirus solutions like Norton 2008-2010 or McAfee 2009-2012 are still being used in many Indian businesses, especially by small businesses and home users. These outdated solutions no longer offer adequate protection against modern cyber threats.

Examples Of Outdated OS Solutions Still Being Used In India

- **Windows Server 2008/2003:** Windows Server 2008 and 2003 are still being used in some Indian organizations. However, both have reached their end-of-life dates (2008 in January 2020 and 2003 in July 2015), and their lack of updates leaves them exposed to cyberattacks.

- **Microsoft Internet Explorer (pre-2015 versions):** Internet Explorer versions prior to 2015 (especially versions 8-10) are still in use, despite no longer being supported by Microsoft. Many businesses in India continue to use legacy applications that require Internet Explorer, making them vulnerable to security breaches.

- **Windows Vista:** Though obsolete, some businesses and government institutions in India continue to use Windows Vista due to software compatibility issues. It stopped receiving support in 2017, leaving systems open to unpatched vulnerabilities.

Automatic Updates and Checklist

Most devices and applications can be set up to automatically update which will make it easier to protect your business. When you maintain security updates, you boost your digital immunity against threats such as viruses, spyware, and more.

Just as we discussed creating an inventory for all our devices in the previous module, we must also maintain an inventory of the patches needed and updated for each of the said devices. A device-wise check involves evaluating every device within the organization to ensure all software is up to date, secure, and operating efficiently. This should be done regularly as part of your business's cybersecurity strategy.

Software Updates and Business Security

- **PCs & Laptops:** These are common targets for ransomware and malware attacks. Ensure antivirus software, firewalls, and operating systems are updated.

- **Mobile Devices:** Mobile phones and tablets are increasingly used in business operations, making them attractive targets for hackers. Update mobile operating systems (iOS, Android) and apps regularly to reduce risk.

- **Servers:** Ensure that server operating systems, databases, and application software are updated, as these often hold sensitive customer data.

- **IoT Devices:** Regularly check the firmware and software on IoT devices such as security cameras, smart thermostats, and connected machinery.

Software Updates and Business Security

Use the following checklist to learn how to better protect your business with updates and patches.

- Prioritize Security Patches
- Automate Updates for All Software for All Devices
- Schedule Manual Updates for Systems That Don't Support Automatic Updates
- Maintain an Inventory of Software & Devices
- Conduct Regular Vulnerability Scans
- Test Patches Before Deployment
- Implement Multi-Layered Security
- Ensure Compliance with Local Regulations
- Use Cloud-Based Solutions with Auto-Updates
- Monitor for End-of-Life (EOL) Software & Devices
- Use Middleware or APIs. Plan Gradual Migration to Modern Platforms
- Backup Critical Data Regularly
- Educate Employees on Update & Security Protocols
- Set a Patch Management Schedule
- Review and Update Third-Party Software
- Keep IoT Devices Secure
- Regularly Review Software EOL DatesConduct
- Test Patches Before Deployment
- Backup & Protect Software and System Configurations
- Use Reliable Patch Management Software
- Use Centralised Patch Management Software
- Monitor for Cybersecurity Breaches
- Limit Internet Access for Devices Using Legacy Software
- Consider Virtual Desktop Solutions that Offer Limited Exposure
- Prioritise Patches Based on Severity of the Vulnerabilities They Address
- Do A Criticality Assessment for All Systems to Assign Priority Ratings While Developing an Incident Response Protocol

Q&A
Session

Any questions or thoughts?

Share with us your queries or thoughts before we proceed to Module 4

APAC Cybersecurity Fund

The Asia Foundation

Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at helpline@cyberpeace.net or on WhatsApp at +91 957-00-000-66

Training Module developed under the project **APAC Cybersecurity Fund**

implemented in India by MSME Foundation for MSME Clusters (FMC)

with support from Google.org